19/7/6
)IALOG(R)File 347:JAPIO
c) 2002 JPO & JAPIO. All rts. reserv.

)6745083 **Image available**
·INTRANET* SYSTEM AND METHOD FOR CONTROLLING *SERVER*

)UB. NO.: 2000-330937 [JP 2000330937 A]
)UBLISHED: November 30, 2000 (20001130)
:NVENTOR(s): SHINKAWA TARO
\PPLICANT(s): YASKAWA ELECTRIC CORP
\PPL. NO.: 11-136187 [JP 99136187]
?ILED: May 17, 1999 (19990517)

ABSTRACT

?ROBLEM TO BE SOLVED: To easily increase the scale of the *intranet* system ınd the capacity of contents while maintaining fast access to a :epresentating *server* by providing proxy *servers* between the :epresentating *server* and a terminal device and decentralizing 'authenticating* and access control processes for *users*.

3OLUTION: When a request to browse desirable contents is sent to a proxy 'server* 11 by using the terminal device 13 of a user 15, the proxy 'server* 11 having received the request retrieves the user. Then it is judged whether authenitication and access control information on the user in already registered on the proxy *server* 11. When the user 15 always nakes requests to browse contents through a terminal device 13 under the proxy *server* 11, the *authentication* and access control information on :he *user* 15 is stored in the proxy *server* 11, so it is speedily judged whether or not browsing is allowed; when browsing is allowed, the contents ıre immediately sent to the terminal device 13 of the user 15 from a representating *server* 10 and when not, it is immediately informed that the use is disallowed.

19/7/7
DIALOG(R)File 347:JAPIO

06623473 **Image available**

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－330937
（P2000－330937A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	15/00	310	G06F	15/00	310A　5B075
		330			330B　5B085
	13/00	351		13/00	351Z　5B089
	17/30			15/40	310F
					320B

審査請求　未請求　請求項の数2　OL　（全 6 頁）

(21)出願番号　特願平11－136187

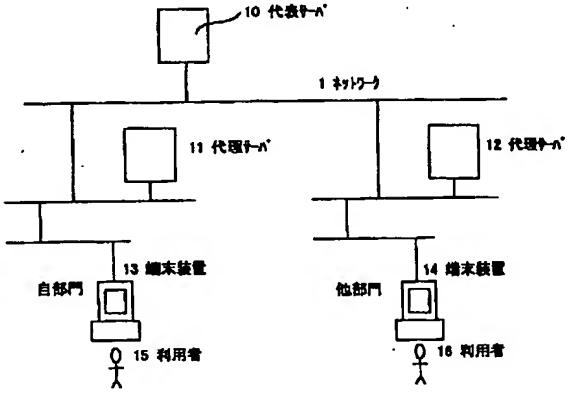
(22)出願日　平成11年５月17日(1999.5.17)

(71)出願人　000006622
株式会社安川電機
福岡県北九州市八幡西区黒崎城石２番１号
(72)発明者　新川　太郎
福岡県北九州市八幡西区黒崎城石２番１号
株式会社安川電機内

Ｆターム(参考)　5B075 KK02 KK43 KK63
5B085 AE23 BG07
5B089 GA11 GA19 HA10 JA22 KA06
KA17 KB13 KC44 KC58 MA03

(54)【発明の名称】　イントラネットシステム及びサーバの制御方法

(57)【要約】
【課題】　イントラネットの大規模化とサーバのコンテンツの大容量化を可能にする。
【解決手段】サーバと端末装置がネットワーク１で接続されたイントラネットシステムに、端末装置１３から閲覧可能な情報を格納した代表サーバ１０と、利用者１５が端末装置１３を用いて代表サーバ１０の情報を閲覧する時は、その閲覧要求を受けて利用者１５の認証をし、認証にパスしたら閲覧要求された情報が利用可能かどうかを判断し、利用可能であれば代表サーバ１０に情報の提供を要求し、利用可能でない場合と認証にパスしない場合はその旨利用者１５に伝える代理サーバ１１とを備える。



1

【特許請求の範囲】

【請求項１】サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、
前記端末装置から閲覧可能な情報を格納した代表サーバと、
利用者が前記端末装置を用いて前記代表サーバの情報を閲覧する時は、その閲覧要求を受けて利用者の認証をし、認証にパスしたら閲覧要求された情報が利用可能かどうかを判断し、利用可能であれば前記代表サーバに情報の提供を要求し、利用可能でない場合と認証にパスしない場合はその旨利用者に伝える代理サーバとを備えたことを特徴とするイントラネットシステム。

【請求項２】代表サーバと代理サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記代表サーバと前記代理サーバとが次の処理を行うよう制御されることを特徴とするサーバの制御方法。

（１）代理サーバが利用者の閲覧要求を受けると、利用者検索をする。

（２）代理サーバは、利用者の認証・アクセス制御情報が代理サーバに登録済みかどうかを判断する。登録済みの場合は（３）に移行し、そうでない場合は（５）に移行する。

（３）代理サーバは要求された情報が閲覧可能かどうかを検査し、可能であれば

（４）に移行し、可能でなければ（９）に移行する。

（４）代表サーバが情報を利用者の端末装置に送り、処理を終了する。

（５）代理サーバが代表サーバに利用者の認証・アクセス制御情報を要求して受けとり、代表サーバが利用者の認証・アクセス制御情報の所在情報を検査する。

（６）代表サーバに代理サーバの、利用者の認証・アクセス制御情報の所在情報があるかどうかを判断し、ない場合は（７）に移行し、ある場合は（８）に移行する。

（７）代表サーバが利用者の認証・アクセス制御情報の所在情報を格納して（３）に移行する。

（８）代表サーバが代理サーバに指示して利用者の認証・アクセス制御情報を破棄させ、（７）に移行する。

（９）代理サーバが利用者にパスワードを入力させて認証情報と比較する。

（１０）利用者の認証にパスすれば（４）に移行し、パスしなければ（１１）に移行する。

（１１）代理サーバは情報を閲覧できないことを利用者に伝え、処理を終了する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、組織内で利用されるイントラネットサーバの認証とアクセス制御の負荷を分散させ、サーバへのアクセスを高速化するイントラネットシステムとサーバの制御方法に関する。

2

【０００２】

【従来の技術】情報伝達の速さや、情報の共有など多くの利点から企業などの組織体でイントラネットが普及しつつある。その接続形態は図７に示すように、イントラネットサーバ７０がネットワーク１を介して多数の端末装置７１、７２、７３、７３…に接続されるというものである。イントラネットサーバ７０には様々な情報が格納されており、ブラウザを使って端末装置７１、７２、７３、７３…から閲覧することができるようになっている。イントラネットサーバ７０に格納されている情報には、人事情報や、財務情報、各種の報告書類等、無差別には公開されていない特定の情報もあり、アクセス制限が施されている。利用者がそれらの情報を閲覧する際は、イントラネットサーバ７０が利用者の認証を行い、その後、閲覧許可のある情報だけを提供するというアクセス制御処理をしている。こうして、閲覧可能な情報だけが閲覧許可のある利用者に提供されるようになっている。

【０００３】

【発明が解決しようとする課題】ところが、イントラネットが大規模になり、端末装置の数とイントラネットサーバに蓄積する情報の量が増えてくると、利用者の認証とアクセス制御を行うイントラネットサーバの負荷が増大し、アクセスする際の所用時間が著しく長くなったり、接続がうまく行かなくなったりすることが多発するなど、イントラネットの利用状況に重大な影響を与えるようになっている。これを回避するには、いっそう高性能なイントラネットサーバの導入が必要となり、コストアップを招いていた。

【０００４】

【課題を解決するための手段】上記問題を解決するため、本発明は、サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記端末装置から閲覧可能な情報を格納した代表サーバと、利用者が前記端末装置を用いて前記代表サーバの情報を閲覧する時は、その閲覧要求を受けて利用者の認証をし、認証にパスしたら閲覧要求された情報が利用可能かどうかを判断し、利用可能であれば前記代表サーバに情報の提供を要求し、利用可能でない場合と認証にパスしない場合はその旨利用者に伝える代理サーバとを備えたことを特徴としている。また本発明のサーバの制御方法は、代表サーバと代理サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記代表サーバと前記代理サーバとが次の処理を行うよう制御されることを特徴とするサーバの制御方法。

（１）代理サーバが利用者の閲覧要求を受けると、利用者検索をする。

（２）代理サーバは、利用者の認証・アクセス制御情報が代理サーバに登録済みかどうかを判断する。登録済みの場合は（３）に移行し、そうでない場合は（５）に移

行する。
（３）代理サーバは要求された情報が閲覧可能かどうかを検査し、可能であれば（４）に移行し、可能でなければ（９）に移行する。
（４）代表サーバが情報を利用者の端末装置に送り、処理を終了する。
（５）代理サーバが代表サーバに利用者の認証・アクセス制御情報を要求して受けとり、代表サーバが利用者の認証・アクセス制御情報の所在情報を検査する。
（６）代表サーバに代理サーバの、利用者の認証・アクセス制御情報の所在情報があるかどうかを判断し、ない場合は（７）に移行し、ある場合は（８）に移行する。
（７）代表サーバが利用者の認証・アクセス制御情報の所在情報を格納して（３）に移行する。
（８）代表サーバが代理サーバに指示して利用者の認証・アクセス制御情報を破棄させ、（７）に移行する。
（９）代理サーバが利用者にパスワードを入力させて認証情報と比較する。
（１０）利用者の認証にパスすれば（４）に移行し、パスしなければ（１１）に移行する。
（１１）代理サーバは情報を閲覧できないことを利用者に伝え、処理を終了する。
【０００５】
【発明の実施の形態】以下、本発明の実施の形態を図に基づいて説明する。図１は本発明のイントラネットシステムの接続形態を示す図であり、図２はその補足説明図、図３、図４、図５はそれぞれ代表サーバと代理サーバ、端末装置の構成を示す図である。図１、図２において、１はネットワーク、１０、２０は代表サーバ、１１、１２、２１、２２は代理サーバ、１３、１４、２３、２４は端末装置、１５、１６、２５は利用者である。代理サーバ１１、１２、２１、２２は、部門サーバなど、他の機能を兼ねる計算機であっても良いし、パソコン等の利用者端末を代用しても良い。
【０００６】図３において、代表サーバは記憶装置３０と演算装置３１、通信装置３２とを備えており、記憶装置３０にはコンテンツ３３、コンテンツアクセス制御データベース３４、ユーザ認証用データベース３５、ユーザ認証情報所在データベース３６が格納されている。コンテンツ３３は利用者が閲覧することができる情報、コンテンツアクセス制御データベース３４はコンテンツ３３が閲覧可能かどうかの情報を含むデータベース、ユーザ認証用データベース３５はユーザの認証に使われる情報を含むデータベース、ユーザ認証情報所在データベース３６はユーザ認証情報がどこにあるかという情報を含むデータベースである。通信装置３２はネットワーク１と演算装置３１に接続されており、ネットワーク１を介して外部の機器と通信する機能を有している。演算装置３１は、情報の入出力や認証などの制御をする機能を有している。ネットワーク１と通信装置３２を使って代理サーバと通信するときは、記憶装置３０のコンテンツアクセス制御データベース３４、ユーザ認証用データベース３５、ユーザ認証情報所在データベース３６を参照して通信制御し、コンテンツ３３を送信して良いと判断したときは通信装置３２に送信指令を与える。
【０００７】代理サーバ１１は記憶装置４０と演算装置４１、通信装置４２とを備えており、記憶装置４０にはコンテンツアクセス制御データベースキャッシュ４３、ユーザ認証用データベースキャッシュ４４が格納されている。コンテンツアクセス制御データベースキャッシュ４３は代表サーバのコンテンツ３３がアクセスされる際に参照されるキャッシュ、ユーザ認証用データベースキャッシュ４４はユーザの認証をする際に参照されるキャッシュである。通信装置４２はネットワーク１と演算装置４１に接続されており、ネットワーク１を介して外部の機器と通信する機能を有している。演算装置４１は、情報の入出力や認証などの制御をする機能を有している。ネットワーク１と通信装置４２を使って代表サーバ及び端末装置と通信するときは、コンテンツアクセス制御データベースキャッシュ４３とユーザ認証用データベースキャッシュ４４を参照して通信制御し、代表サーバにコンテンツ３３の送信の可否を伝える機能を有している。
【０００８】端末装置１３は記憶装置５０と演算装置５１、通信装置５２とを備えており、記憶装置５０には汎用ブラウザソフトウェア５３が格納されている。汎用ブラウザソフトウェア５３は代表サーバのコンテンツ３３を閲覧する機能を備えたツールである。通信装置５２はネットワーク１と演算装置５１に接続されており、ネットワーク１を介して外部の機器と通信する機能を有している。演算装置５１は、情報の入出力や認証の要求をする機能を有している。汎用ブラウザソフトウェア５３が起動すると、ネットワーク１と通信装置５２を使って代理サーバで認証を受け、認証にパスしてコンテンツ３３が閲覧可能であればコンテンツ３３を受信して閲覧することができる。
【０００９】図１の接続形態をしたイントラネットシステムで利用者１５が代表サーバ１０に格納されている情報を閲覧するときは、イントラネットシステムは図６のフローチャートに沿って動作する。この図において、まず（Ｓ１）で利用者１５が端末装置１３を使って代理サーバ１１に閲覧したいコンテンツ３３の閲覧要求をすると、（Ｓ２）で閲覧要求を受けた代理サーバ１１が利用者の検索をする。そして（Ｓ３）で代理サーバ１１は利用者の認証・アクセス制御情報が代理サーバ１１に登録済みかどうかを判断し、登録済みであれば（Ｓ４）に移行して、そうでなければ（Ｓ７）に移行する。（Ｓ４）では代理サーバ１１が、代表サーバ１０のコンテンツ３３が参照可能かどうかを検査する。その結果、（Ｓ５）利用者が代表サーバ１０のコンテンツ３３を閲覧するこ

とが可能と判断されれば（Ｓ６）に移行し、そうでなければ（Ｓ１４）に移行する。（Ｓ７）では代理サーバ１１が代表サーバ１０に利用者１５の認証・アクセス制御情報を要求し、（Ｓ８）その要求を受けた代表サーバ１０が代理サーバ１１に利用者１５の認証・アクセス制御情報を伝え、同時に（Ｓ９）利用者１５の認証・アクセス制御情報の所在情報を検査する。そして（Ｓ１０）代表サーバに代理サーバの利用者１５の認証・アクセス制御情報の所在情報がなければ（Ｓ１３）に移行し、そうでなければ（Ｓ１１）に移行する。（Ｓ１１）では、代表サーバ１０は利用者１５の認証・アクセス制御情報を破棄するよう代理サーバ１１に通知し、（Ｓ１２）代理サーバ１１が該当する情報を破棄して（Ｓ１３）に移行する。（Ｓ１３）では、代表サーバ１０は利用者１５の認証・アクセス制御情報の所在情報を記憶装置３０に格納して（Ｓ４）に移行する。（Ｓ１４）では、代理サーバ１１が利用者１５の認証をし、（Ｓ１５）認証にパスしたと判断したら（Ｓ６）に移行し、そうでなければ（Ｓ１６）に移行する。（Ｓ１６）では、代理サーバ１１は、利用者１５が使っている端末装置１３に、利用者１５が代表サーバ１０のコンテンツ３３を閲覧できないということを通知して、処理を終了する。（Ｓ６）では、代表サーバ１０がコンテンツ３３を利用者１５が使っている端末装置１３に送信して処理を終了する。

【００１０】上記の手順でイントラネットシステムが動作しているため、利用者１５が常に代理サーバ１１の下位にある端末装置１３でコンテンツ３３の閲覧要求をするときは、利用者１５の認証・アクセス制御情報が代理サーバ１１に格納されているので、代理サーバ１１で閲覧の可否が速やかに判断され、閲覧可能な場合はすぐに代表サーバ１０からコンテンツ３３が利用者１５の端末装置１３に送信され、そうでない場合は利用できないことがすぐに通知される。また、図2のように、利用者２５が通常とは異なる代理サーバ２２の下位にある端末装置２４を使って閲覧要求をするときは、代理サーバ２２が代表サーバ２０から利用者２５のユーザ認証所在情報を得るとともに、代表サーバ２０が代理サーバ２１に蓄えられている利用者２５の認証・アクセス制御情報を廃棄させるので、認証・アクセス制御情報を速やかに書き換えることができ、閲覧可能かどうかの判断も速やかにできるのである。

【００１１】このように、代表サーバの下位にある全ての利用者の認証・アクセス制御情報が代表サーバで一元管理されているとともに、利用者が同じ代理サーバを使

って閲覧要求をする限り、その代理サーバによって全ての認証・アクセス制御が行われる。上記のほか、代表サーバで管理されている利用者の認証・アクセス制御情報に変更があった場合には、直前に認証作業をした代理サーバが蓄積している利用者の認証・アクセス制御情報が更新され、最新の認証・アクセス制御情報が保持される。

【００１２】

【発明の効果】以上述べたように、本発明によれば、代表サーバと端末装置の間に複数の代理サーバを設けてユーザの認証・アクセス制御処理を分散させ、代表サーバに認証・アクセス制御情報の一元管理をさせているので、代表サーバへのアクセスの高速性を維持しつつイントラネットシステムの大規模化とコンテンツの大容量化を容易にすることができるという実用的効果がある。

【図面の簡単な説明】

【図１】　本発明のイントラネットシステムの接続形態図

【図２】　補足説明図

【図３】　代表サーバの構成図

【図４】　代理サーバの構成図

【図５】　端末装置の構成図

【図６】　本発明の処理手順を示すフローチャート

【図７】　従来のイントラネットシステムの接続形態図

【符号の説明】

１　ネットワーク

１０、２０　代表サーバ

１１、１２、２１、２２　代理サーバ

１３、１４、２３、２４、７１、７２、７３、７４　端末装置

１５、１６、２５　利用者

３０、４０、５０　記憶装置

３１、４１、５１　演算装置

３２、４２、５２　通信装置

３３　コンテンツ

３４　コンテンツアクセス制御データベース

３５　ユーザ認証用データベース

３６　ユーザ認証情報所在データベース

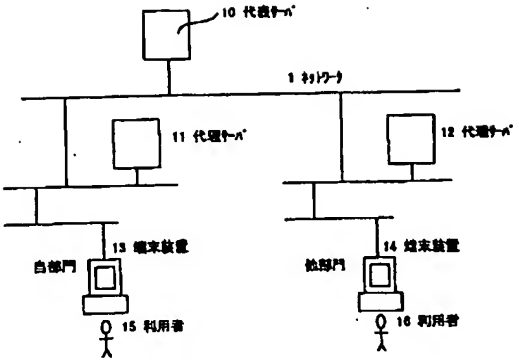
４３　コンテンツ・アクセス制御データベースキャッシュ

４４　ユーザ認証用データベースキャッシュ

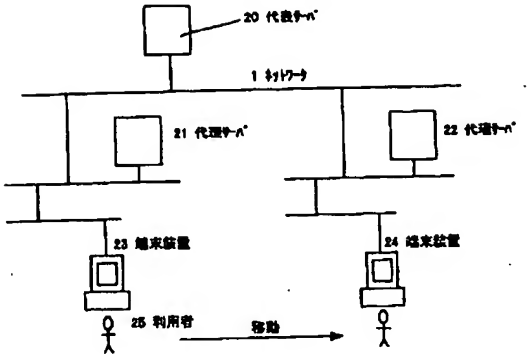
５３　汎用ブラウザソフトウェア

７０　イントラネットサーバ

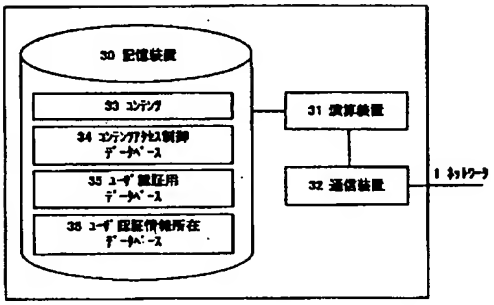
【図１】



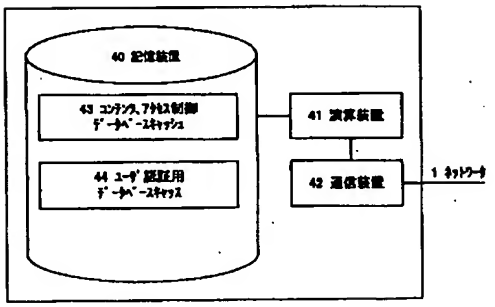
【図２】



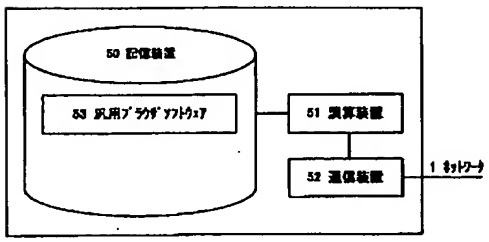
【図３】



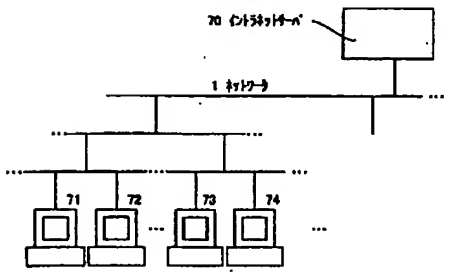
【図４】



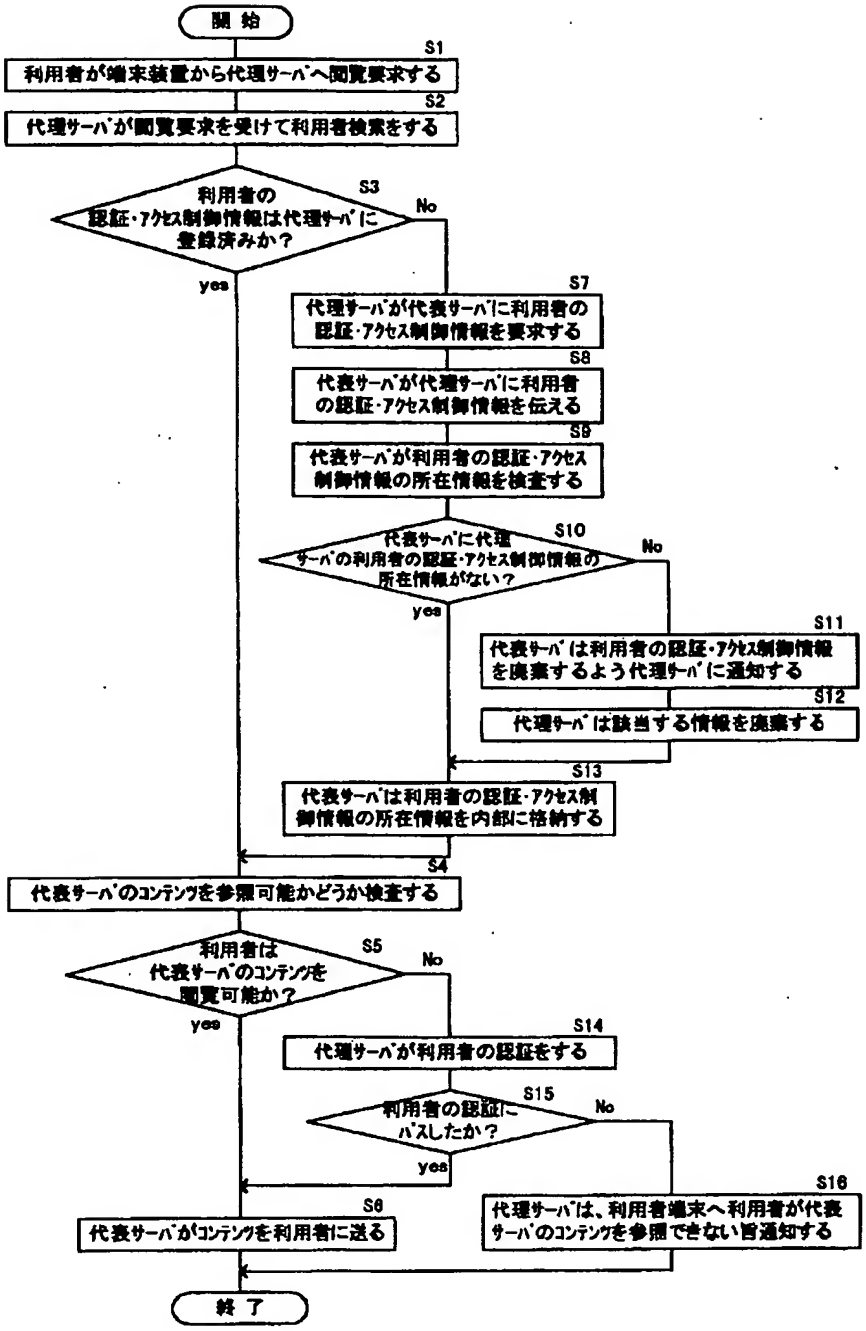
【図５】



【図７】



【図６】


開始
S1
利用者が端末装置から代理ｻｰﾊﾞへ閲覧要求する
S2
代理ｻｰﾊﾞが閲覧要求を受けて利用者検索をする
S3
利用者の認証・ｱｸｾｽ制御情報は代理ｻｰﾊﾞに登録済みか？
No
yes
S7
代理ｻｰﾊﾞが代表ｻｰﾊﾞに利用者の認証・ｱｸｾｽ制御情報を要求する
S8
代表ｻｰﾊﾞが代理ｻｰﾊﾞに利用者の認証・ｱｸｾｽ制御情報を伝える
S9
代表ｻｰﾊﾞが利用者の認証・ｱｸｾｽ制御情報の所在情報を検査する
S10
代表ｻｰﾊﾞに代理ｻｰﾊﾞの利用者の認証・ｱｸｾｽ制御情報の所在情報がない？
No
yes
S11
代表ｻｰﾊﾞは利用者の認証・ｱｸｾｽ制御情報を廃棄するよう代理ｻｰﾊﾞに通知する
S12
代理ｻｰﾊﾞは該当する情報を廃棄する
S13
代表ｻｰﾊﾞは利用者の認証・ｱｸｾｽ制御情報の所在情報を内部に格納する
S4
代表ｻｰﾊﾞのｺﾝﾃﾝﾂを参照可能かどうか検査する
S5
利用者は代表ｻｰﾊﾞのｺﾝﾃﾝﾂを閲覧可能か？
No
yes
S14
代理ｻｰﾊﾞが利用者の認証をする
S15
利用者の認証にﾊﾟｽしたか？
No
yes
S16
代理ｻｰﾊﾞは、利用者端末へ利用者が代表ｻｰﾊﾞのｺﾝﾃﾝﾂを参照できない旨通知する
S6
代表ｻｰﾊﾞがｺﾝﾃﾝﾂを利用者に送る
終了